MAGNET FORENSICS®

Von Alerts Zu Entscheidungen

Die neue Realität des DFIR in einer Welt, in der Ermittlungen das Geschäftsrisiko bestimmen

[02:47 UHR · ENTERPRISE]

Ein Alert. Severity: Critical.

CISO schreibt:
"Was ist passiert?"

Das Board will bis 08:00 eine Antwort.
Vollständig. Belastbar. Entscheidungsfähig.

Drei unvollständige Tools.

Kein Remote-Zugriff auf zwei Endpoints.

Logs aus fünf Quellen. Keine gemeinsame Plattform.

Sind Sie bereit, dem Board zu antworten?

oder

[05:30 UHR · STRAFVERFOLGUNG]

Sichergestelltes Gerät. Tatvorwurf: schwer.

Staatsanwalt fragt:
"Was stand auf dem Handy?"

Anhörung in 24 Stunden.
Die Extraktion muss gerichtsverwertbar sein.

Gerät gesperrt. Passcode bekannt

Messenger-Daten verschlüsselt -Cloud-Backup unvollständig.

Fünf Geräte sichergestellt. Ein Forensiker. 24 Stunden.

Sind Sie bereit für die Anhörung?

Zwei Welten. Dieselbe Herausforderung:

Aus Daten eine entscheidungsfähige Antwort machen … schnell, belastbar, für jeden Stakeholder.

Solutions Consultant
Since May 2022

Technical Pre-Sales
March 2018 – April 2022

Workgroup-Server Engineer
High-End Server Engineer
Systems Support Professional - Santa Clara, CA USA
(5yrs on intl. assignment)
Principal Support Engineer f. Cloud systems
March 2001 – Feb. 2018

User Help Desk for Sun Microsystems
High-End Server remote monitoring
March 2000 – Feb. 2001

System Engineer
Windows, Linux, Novell-Network
June 1999 – Dec. 1999

DST - Dieckmann Systemtechnik GmbH

Niels Renken

Solutions Consultant, EMEA

niels.renken@magnetforensics.com

AGENDA

Was Sie heute erwartet

01 **Die neue Realität des DFIR**

Warum die Erwartungen steigen, global und im DACH-Raum

02 **DACH-Lagebild**

BSI & Bitkom: Was das für deutsche Unternehmen bedeutet

03 **Zenario #1: DFIR als strategischer Risikofaktor**

Unverzichtbare Kompetenzen, unterschätzter Wert

04 **#2 & #3: Remote, Mobile & interne Hindernisse**

71 % kämpfen mit Remote-Erfassung. Burnout wächst

05 **Befund #4 + Ausblick 2026: KI & SaaS**

Von 21 % auf 94 % … und was 2026 neu dazukommt

06 **Empfehlungen & Diskussion**

Was DFIR-Teams jetzt tun müssen

KONTEXT

Die neue Realität des DFIR

Mehr Vorfälle

Phishing, Ransomware und Cybercrime nehmen zu, für Unternehmen und Strafverfolgungsbehörden gleichzeitig.

+37 %

Ransomware YoY
(Verizon DBIR 2025)

Höherer Impact

Cyberangriffe sind Vorstandsthemen und Staatsanwaltschaftsfälle. Belastbare Erkenntnisse zählen überall.

$4,44 Mio.

Ø Schadenskosten
pro Datenpanne (IBM 2025)

Höhere Erwartungen

Boards, Regulatoren, Richter und Behörden: Alle verlangen schnellere, gerichtsverwertbare Antworten.

94 %

der Cyber-Leader:
KI wird Kraft Nr. 1 (WEF 2026)

Quellen: Verizon Data Breach Investigations Report 2025 · IBM Cost of a Data Breach 2025 · World Economic Forum Global Cybersecurity Outlook 2026

DACH-LAGEBILD · CORPORATE & BEHÖRDEN

Was das für Deutschland bedeutet

202,4 Mrd. €

Schaden durch Cyber-angriffe in Deutschland

70 % des Gesamtschadens von 289,2 Mrd. €

Bitkom Wirtschaftsschutz 2025

87 %

der deutschen Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen

Bitkom 2025

950

Ransomware-Angriffe auf dt. Unternehmen & Behörden im Berichtszeitraum 2024/25

BSI Lagebericht 2025

119 / Tag

neu entdeckte Schwachstellen in Deutschland, +24 % YoY

BSI Lagebericht 2025

56 %

KMU erfüllen nur 56 % der IT-Sicherheits-Basisanforderungen, leichtes Ziel

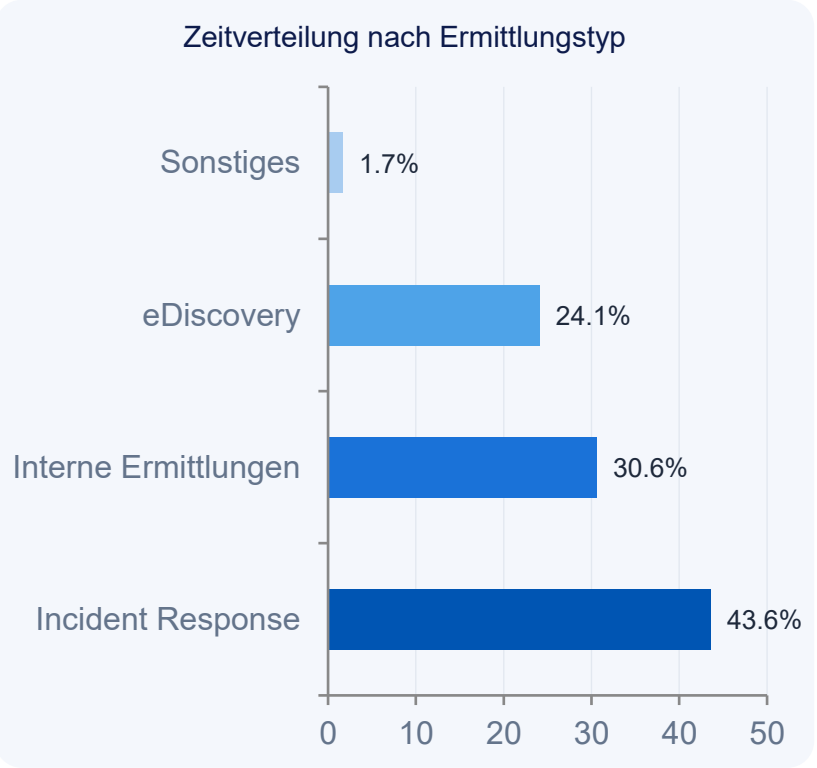
BSI Lagebericht 2025

BSI 2025: "Die Gesamtlage ist nach wie vor angespannt." - Gilt für Unternehmen und Behörden gleichermassen.

#1

DFIR als strategischer Risikofaktor

1. 43,6 % der Zeit auf Incident Response, gefolgt von internen Ermittlungen (30,6 %) und eDiscovery (24,1 %).
2. Phishing/BEC und Ransomware führen die Häufigkeitsliste an, Compliance-Ermittlungen folgen auf Platz 3.
3. 49 % der Unternehmen lagern DFIR-Aktivitäten aus, primär für Unparteilichkeit und Kapazität.
4. 72 % sagen: Management erkennt DFIR-Wert an (↓ von 83 %). 68 % fühlen sich ausreichend ausgestattet (↓ von 77 %).



Verizon DBIR 2025: 3rd-Party-Beteiligung bei Datenpannen verdoppelt (15 % → 30 %), DFIR-Fähigkeiten werden zum Differenzierungsmerkmal.

⚠ Rückgang 83 % → 72 %: Management-Bewusstsein für DFIR sinkt, obwohl die Bedrohungslage steigt.

#2

Remote-Erfassung & mobile Geräte

71 %
berichten: Remote-Erfassung ist ein mittleres bis extremes Problem

64 %
sehen Wachstum hybrider Belegschaften als moderates bis extremes Problem

65,5 %
verzeichnen zunehmend mehr mobile Geräte in Ermittlungen

32 %
erwarten: mobile Geräte machen DFIR künftig noch schwieriger (↑ vs. 26 %)

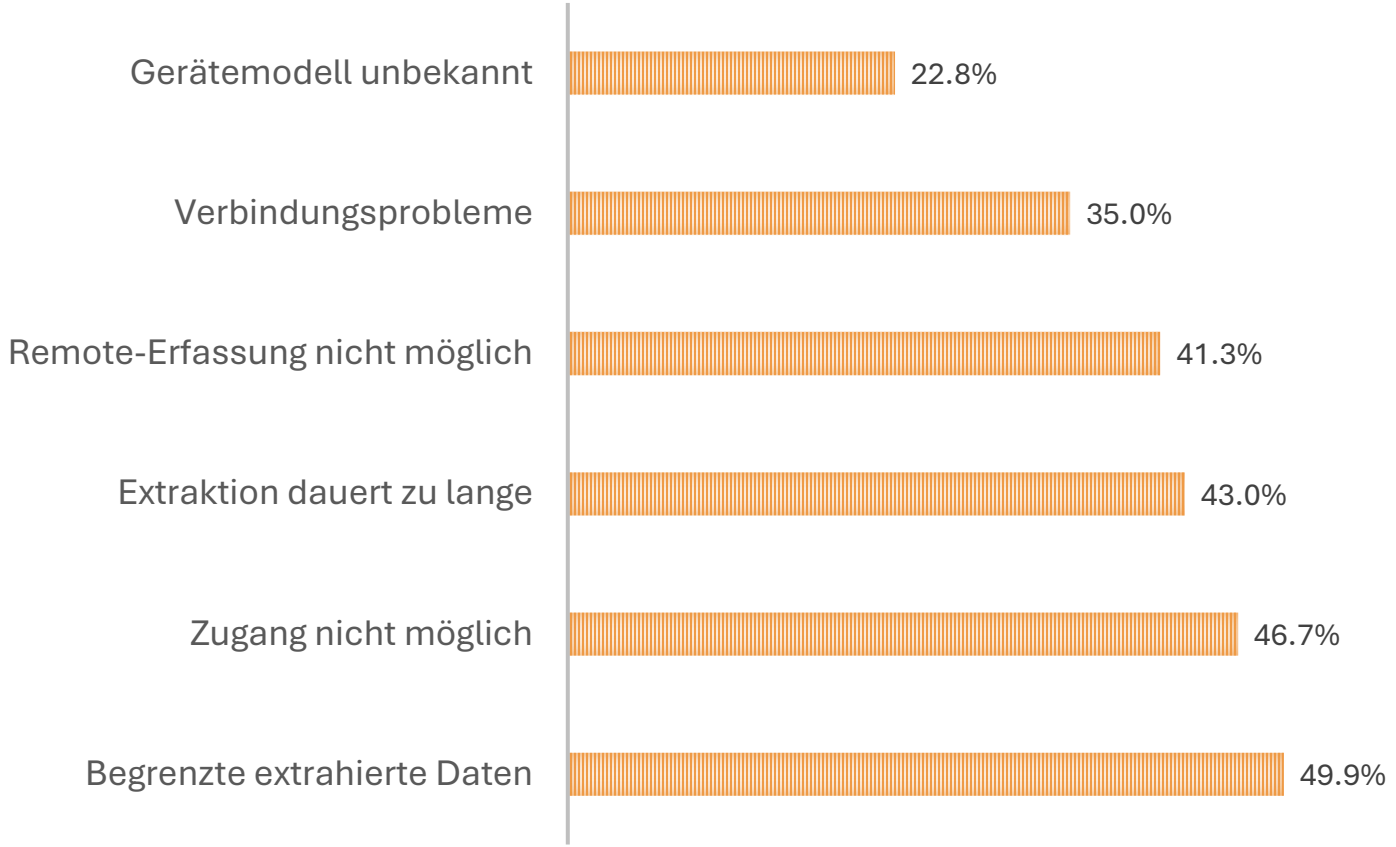
Verizon DBIR 2025: Vulnerability Exploitation +34 % - Zero-Day-Angriffe auf Perimeter-Geräte häufigster Initialkompromiss. BYOD verstärkt die Angriffsfläche.

Moderne Tools für Remote-Erfassung und Full-File-System-Extraktion sind keine Option mehr, sie sind Voraussetzung.

MAGNET FORENSICS®

#2 – DETAIL

Die größten Hürden bei mobilen Geräten



→ Cloud-Backups allein reichen nicht: gelöschte Daten, verschlüsselte Artefakte und App-Daten fehlen. BSI 2025 bestätigt: MDM-Lücken bei BYOD wachsen.

68 %

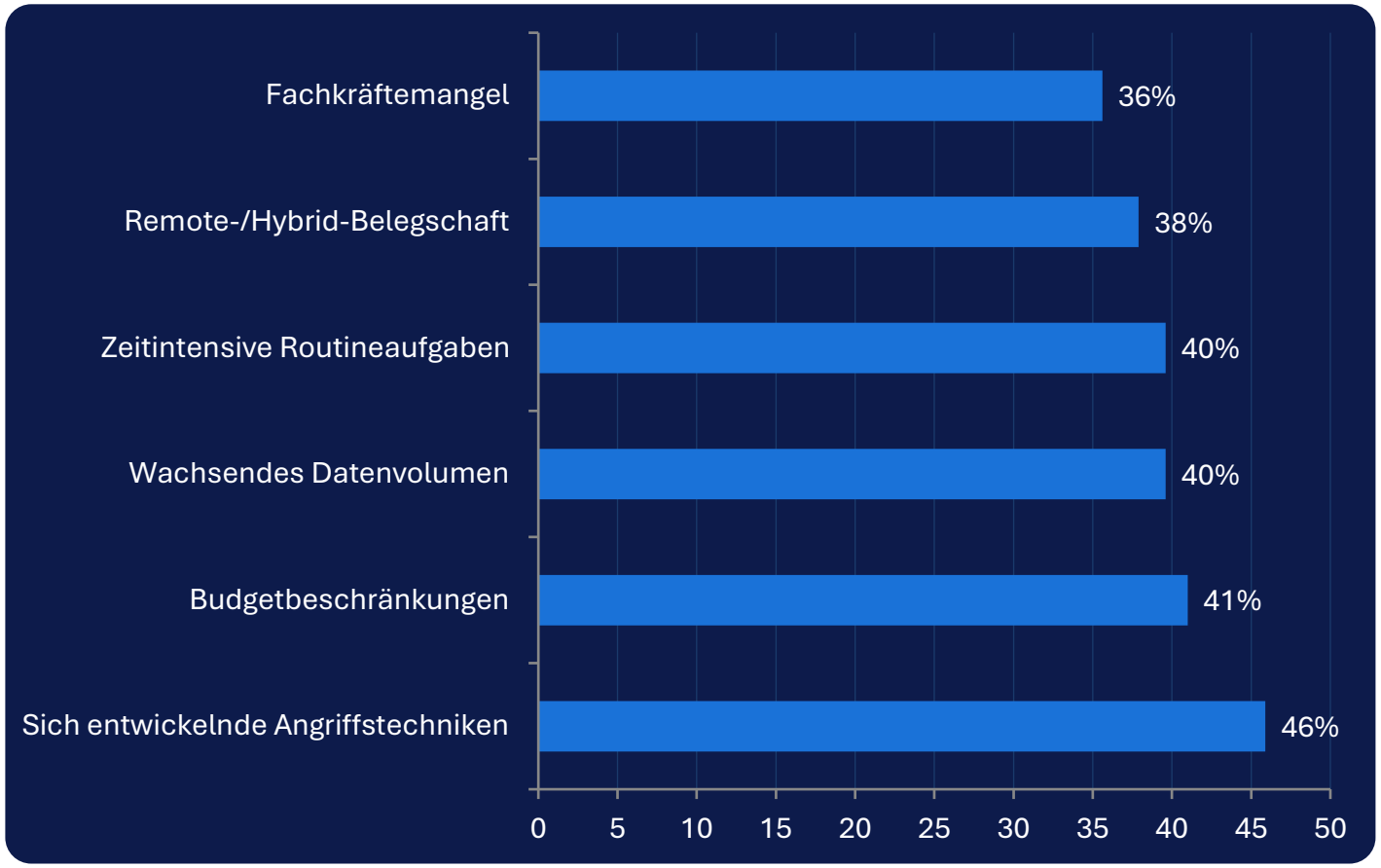
bevorzugen FFS-Extraktion, aber Zugang ist meist das Problem.

56 %

nutzen Mobile-Daten aus forensischen Tools regelmäßig in Ermittlungen.

#3

Interne Hindernisse - die unterschätzte Bremse



39 % fühlen sich ausgebrannt (↑ von 34 % im Vorjahr)

68 % bestätigen: Teams haben die nötigen Ressourcen (↓ von 77 %)

58 % empfinden die Zusammenarbeit mit der IT als mindestens mäßig herausfordernd

3 Jahre in Folge: Angriffstechniken sind die Nr. 1-Herausforderung. Aber Budget, Burnout & IT-Kooperation sind intern lösbar. | Bitkom 2025: Nur 50 % fühlen sich auf Cyberangriffe gut vorbereitet

#4

KI und SaaS transformieren DFIR … Jetzt!

94 %

nutzen KI bereits aktiv in Ermittlungen

vs. nur 21 % im Vorjahr

64,7 % Hochpräzise Datenklassifikation

60,5 % Text- & Bildanalyse

44,4 % Entwurf / Bearbeitung von Berichten

43,8 % Automatische Berichterstellung

79 %

verwenden bereits SaaS-basierte forensische Tools

WEF Global Cybersecurity Outlook 2026:

94 % der Cyber-Führungskräfte erwarten, dass KI die folgenreichste Kraft in der Cybersicherheit 2026 sein wird.

51 % sehen KI als größten Nutzen. **56 %** sehen KI gleichzeitig als größte Herausforderung.

FRISCH ERSCHIENEN

2026 State of Enterprise DFIR - was sich verändert hat

68 %

nutzen KI (2026 Magnet Report)

KI wird zur Pflicht, nicht mehr zur Option

68 % nutzen KI in Ermittlungen (↑ dramatisch von 20 % in 2024). Gleichzeitig nutzen Angreifer KI für raffiniertere Attacken.

+24 %

Collaboration-Treiber YoY

Real-Time Collaboration: neuer Standard

+24 % YoY als Treiber für SaaS-Adoption. 80 % sagen, SaaS hilft Ermittlungen zu skalieren. Collaboration ist kein Nice-to-have mehr.

66 %

mehr Geräte pro Fall

Mobile: unverzichtbar & schwieriger

61 % nutzen Mobile-Daten regelmäßig. 66 % sehen mehr Geräte pro Fall. OS-Sicherheit, Verschlüsselung & MDM erschweren den Zugang weiter.

7,1

Ø Tools / Fall (↑ von 5,5)

Tool-Proliferation: von 5,5 auf 7,1 Tools

Die Anzahl genutzter Tools pro Fall stieg von 5,5 auf 7,1. Mehr Reibung, schlechtere Korrelation, höheres Burnout-Risiko.

Quelle: 2026 State of Enterprise DFIR Report - Magnet Forensics (erschienen März 2026, n > 360 DFIR-Professionals)

MAGNET FORENSICS®

Was DFIR-Teams jetzt tun müssen

1 DFIR als Business-Funktion positionieren

202,4 Mrd. € Schaden in DE (Bitkom 2025). DFIR ist keine Kostenstelle, es ist Risikomanagement.

2 Remote- & Mobile-Fähigkeiten ausbauen

71 % kämpfen mit Remote-Erfassung. Tools müssen remote-first sein und FFS-Extraktion ermöglichen.

3 Interne Silos & Burnout-Risiken angehen

39 % fühlen sich ausgebrannt. IT-Kooperation und Automatisierung sind keine Luxus-Optionen.

4 KI & SaaS strategisch nutzen

Von 21 % → 94 % in einem Jahr. Tool-Proliferation (7,1/Fall) aktiv managen.

Wie Magnet Forensics unterstützt

MAGNET AXIOM CYBER™

Remote-Erfassung und Analyse über Computer, Cloud, IoT und Mobile, alles in einer Lösung.

Remote · Cloud · Mobile

MAGNET NEXUS™

Endpoint-Erfassung und Analyse in Echtzeit - skalierbar, kollaborativ, schnell. Löst das 71%-Problem.

Speed · Scale · Collaboration

MAGNET VERAKEY™

Consent-basierte mobile Forensik mit FFS-Extraktion. Antwortet direkt auf die mobile DACH-Herausforderung.

Mobile · FFS · Compliance

MAGNET AUTOMATE™

Automatisierte Erfassung, Verarbeitung & Reporting. Eliminiert Routineaufgaben, von Stunden zu Minuten. weniger Tools, mehr Klarheit.

Automation · Playbooks · Scale

Sprechen Sie uns an. Wir zeigen Ihnen, wie DFIR schneller, smarter und skalierbarer wird.

State of Enterprise DFIR **2026 Report**

Learn more about trends and challenges shaping digital investigations, and how to shape your strategy for the year ahead.

Fragen & Diskussion

Quellen dieser Präsentation:

Magnet Forensics: 2025 & 2026 State of Enterprise DFIR Report
BSI: Lagebericht IT-Sicherheit Deutschland 2025
Bitkom: Wirtschaftsschutz 2025 Verizon: Data Breach Investigations Report 2025
IBM: Cost of a Data Breach 2025
WEF: Global Cybersecurity Outlook 2026

Read the report

State of Enterprise DFIR **2026 Report**

And lets connect:

After this presentation at our booth,

via Email:
Niels.Renken@magnetforensics.com,

Via LinkedIn:
https://www.linkedin.com/in/nielsrenken